STANDARDVERTRAGSKLAUSELN - AVV

VIDEC Data Engineering GmbH
Stand 10.2026 (V26.10-01)

I. ABSCHNITT I

1. Klausel 1: Zweck und Anwendungsbereich

a) Mit diesen Standardvertragsklauseln (im Folgenden „Klauseln") soll die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sichergestellt werden.

b) Die in Anhang I aufgeführten Verantwortlichen und Auftragsverarbeiter haben diesen Klauseln zugestimmt, um die Einhaltung von Artikel 28 Absätze 3 und 4 der Verordnung (EU) 2016/679 und/oder Artikel 29 Absätze 3 und 4 der Verordnung (EU) 2018/1725 zu gewährleisten.

c) Diese Klauseln gelten für die Verarbeitung personenbezogener Daten gemäß Anhang II.

d) Die Anhänge I bis IV sind Bestandteil der Klauseln.

e) Diese Klauseln gelten unbeschadet der Verpflichtungen, denen der Verantwortliche gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

f) Diese Klauseln stellen für sich allein genommen nicht sicher, dass die Verpflichtungen im Zusammenhang mit internationalen Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 erfüllt werden.

2. Klausel 2: Unabänderbarkeit der Klauseln

a) Die Parteien verpflichten sich, die Klauseln nicht zu ändern, es sei denn, zur Ergänzung oder Aktualisierung der in den Anhängen angegebenen Informationen.

b) Dies hindert die Parteien nicht daran die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen und weitere Klauseln oder zusätzliche Garantien hinzuzufügen, sofern diese weder unmittelbar noch mittelbar im Widerspruch zu den Klauseln stehen oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

3. Klausel 3: Auslegung

a) Werden in diesen Klauseln die in der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 definierten Begriffe verwendet, so haben diese Begriffe dieselbe Bedeutung wie in der betreffenden Verordnung.

b) Diese Klauseln sind im Lichte der Bestimmungen der Verordnung (EU) 2016/679 bzw. der Verordnung (EU) 2018/1725 auszulegen.

c) Diese Klauseln dürfen nicht in einer Weise ausgelegt werden, die den in der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 vorgesehenen Rechten und Pflichten zuwiderläuft oder die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneidet.

4. Klausel 4: Vorrang

Im Falle eines Widerspruchs zwischen diesen Klauseln und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den Parteien bestehen oder später eingegangen oder geschlossen werden, haben diese Klauseln Vorrang.

5. Klausel 5: Kopplungsklausel

a) Eine Einrichtung, die nicht Partei dieser Klauseln ist, kann diesen Klauseln mit Zustimmung aller Parteien jederzeit als Verantwortlicher oder als Auftragsverarbeiter beitreten, indem sie die Anhänge ausfüllt und Anhang I unterzeichnet.

b) Nach Ausfüllen und Unterzeichnen der unter Buchstabe a genannten Anhänge wird die beitretende Einrichtung als Partei dieser Klauseln behandelt und hat die Rechte und Pflichten eines Verantwortlichen oder eines Auftragsverarbeiters entsprechend ihrer Bezeichnung in Anhang I.

c) Für die beitretende Einrichtung gelten für den Zeitraum vor ihrem Beitritt als Partei keine aus diesen Klauseln resultierenden Rechte oder Pflichten.

II. ABSCHNITT II

PFLICHTEN DER PARTEIEN

6. Klausel 6: Beschreibung der Verarbeitung

Die Einzelheiten der Verarbeitungsvorgänge, insbesondere die Kategorien personenbezogener Daten und die Zwecke, für die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden, sind in Anhang II aufgeführt.

7. Klausel 7: Pflichten der Parteien

7.1. Weisungen

a) Der Auftragsverarbeiter verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Verantwortliche kann während der gesamten Dauer der Verarbeitung personenbezogener Daten weitere Weisungen erteilen. Diese Weisungen sind stets zu dokumentieren.

b) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass vom Verantwortlichen erteilte Weisungen gegen die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder geltende Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstoßen.

7.2. Zweckbindung

Der Auftragsverarbeiter verarbeitet die personenbezogenen Daten nur für den/die in Anhang II genannten spezifischen Zweck(e), sofern er keine weiteren Weisungen des Verantwortlichen erhält.

7.3. Dauer der Verarbeitung personenbezogener Daten

Die Daten werden vom Auftragsverarbeiter nur für die in Anhang II angegebene Dauer verarbeitet.

7.4. Sicherheit der Verarbeitung

a) Der Auftragsverarbeiter ergreift mindestens die in Anhang III aufgeführten technischen und organisatorischen Maßnahmen, um die Sicherheit der personenbezogenen Daten zu gewährleisten. Dies umfasst den Schutz der Daten vor einer Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu den Daten führt (im Folgenden „Verletzung des Schutzes

personenbezogener Daten"). Bei der Beurteilung des angemessenen Schutzniveaus tragen die Parteien dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie den für die betroffenen Personen verbundenen Risiken gebührend Rechnung.

b) Der Auftragsverarbeiter gewährt seinem Personal nur insoweit Zugang zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, als dies für die Durchführung, Verwaltung und Überwachung des Vertrags unbedingt erforderlich ist. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der erhaltenen personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.5. Sensible Daten

Falls die Verarbeitung personenbezogene Daten betrifft, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oder die genetische Daten oder biometrische Daten zum Zweck der eindeutigen Identifizierung einer natürlichen Person, Daten über die Gesundheit, das Sexualleben oder die sexuelle Ausrichtung einer Person oder Daten über strafrechtliche Verurteilungen und Straftaten enthalten (im Folgenden „sensible Daten"), wendet der Auftragsverarbeiter spezielle Beschränkungen und/oder zusätzlichen Garantien an.

7.6. Dokumentation und Einhaltung der Klauseln

a) Die Parteien müssen die Einhaltung dieser Klauseln nachweisen können.

b) Der Auftragsverarbeiter bearbeitet Anfragen des Verantwortlichen bezüglich der Verarbeitung von Daten gemäß diesen Klauseln umgehend und in angemessener Weise.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen alle Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesen Klauseln festgelegten und unmittelbar aus der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 hervorgehenden Pflichten erforderlich sind. Auf Verlangen des Verantwortlichen gestattet der Auftragsverarbeiter ebenfalls die Prüfung der unter diese Klauseln fallenden Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung und trägt zu einer solchen Prüfung bei. Bei der Entscheidung über eine Überprüfung oder Prüfung kann der Verantwortliche einschlägige Zertifizierungen des Auftragsverarbeiters berücksichtigen.

d) Der Verantwortliche kann die Prüfung selbst durchführen oder einen unabhängigen Prüfer beauftragen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten oder physischen Einrichtungen des Auftragsverarbeiters umfassen und werden gegebenenfalls mit angemessener Vorankündigung durchgeführt.

e) Die Parteien stellen der/den zuständigen Aufsichtsbehörde(n) die in dieser Klausel genannten Informationen, einschließlich der Ergebnisse von Prüfungen, auf Anfrage zur Verfügung.

7.7. Einsatz von Unterauftragsverarbeitern

a) Der Auftragsverarbeiter besitzt die allgemeine Genehmigung des Verantwortlichen für die Beauftragung von Unterauftragsverarbeitern, die in einer vereinbarten Liste aufgeführt sind. Der Auftragsverarbeiter unterrichtet den Verantwortlichen mindestens 14 Tage im Voraus ausdrücklich in schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Hinzufügen oder Ersetzen von Unterauftragsverarbeitern und räumt dem Verantwortlichen damit ausreichend Zeit ein, um vor der Beauftragung des/der betreffenden Unterauftragsverarbeiter/s Einwände gegen diese Änderungen erheben zu können. Der Auftragsverarbeiter stellt dem Verantwortlichen die erforderlichen Informationen zur Verfügung, damit dieser sein Widerspruchsrecht ausüben kann.

b) Beauftragt der Auftragsverarbeiter einen Unterauftragsverarbeiter mit der Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen), so muss diese Beauftragung im Wege eines Vertrags erfolgen, der dem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auferlegt wie diejenigen, die für den Auftragsverarbeiter gemäß diesen Klauseln gelten. Der Auftragsverarbeiter stellt sicher, dass der Unterauftragsverarbeiter die Pflichten erfüllt, denen der Auftragsverarbeiter entsprechend diesen Klauseln und gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 unterliegt.

c) Der Auftragsverarbeiter stellt dem Verantwortlichen auf dessen Verlangen eine Kopie einer solchen Untervergabevereinbarung und etwaiger späterer Änderungen zur Verfügung. Soweit es zum Schutz von Geschäftsgeheimnissen oder anderen vertraulichen Informationen, einschließlich personenbezogener Daten notwendig ist, kann der Auftragsverarbeiter den Wortlaut der Vereinbarung vor der Weitergabe einer Kopie unkenntlich machen.

d) Der Auftragsverarbeiter haftet gegenüber dem Verantwortlichen in vollem Umfang dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragsverarbeiter geschlossenen Vertrag nachkommt. Der Auftragsverarbeiter benachrichtigt den Verantwortlichen, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

e) Der Auftragsverarbeiter vereinbart mit dem Unterauftragsverarbeiter eine Drittbegünstigtenklausel, wonach der Verantwortliche – im Falle, dass der Auftragsverarbeiter faktisch oder rechtlich nicht mehr besteht oder zahlungsunfähig ist – das Recht hat, den Untervergabevertrag zu kündigen und den Unterauftragsverarbeiter anzuweisen, die personenbezogenen Daten zu löschen oder zurückzugeben.

7.8. Internationale Datenübermittlungen

a) Jede Übermittlung von Daten durch den Auftragsverarbeiter an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Verantwortlichen oder zur Einhaltung einer speziellen Bestimmung nach dem Unionsrecht oder dem Recht eines Mitgliedstaats, dem der Auftragsverarbeiter unterliegt, und muss mit Kapitel V der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 im Einklang stehen.

b) Der Verantwortliche erklärt sich damit einverstanden, dass in Fällen, in denen der Auftragsverarbeiter einen Unterauftragsverarbeiter gemäß Klausel 7.7 für die Durchführung bestimmter Verarbeitungstätigkeiten (im Auftrag des Verantwortlichen) in Anspruch nimmt und diese Verarbeitungstätigkeiten eine Übermittlung personenbezogener Daten im Sinne von Kapitel V der Verordnung (EU) 2016/679 beinhalten, der Auftragsverarbeiter und der Unterauftragsverarbeiter die Einhaltung von Kapitel V der Verordnung (EU) 2016/679 sicherstellen können, indem sie Standardvertragsklauseln verwenden, die von der Kommission gemäß Artikel 46 Absatz 2 der Verordnung (EU) 2016/679 erlassen wurden, sofern die Voraussetzungen für die Anwendung dieser Standardvertragsklauseln erfüllt sind.

8. Klausel 8: Unterstützung des Verantwortlichen

a) Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich über jeden Antrag, den er von der betroffenen Person erhalten hat. Er beantwortet den Antrag nicht selbst, es sei denn, er wurde vom Verantwortlichen dazu ermächtigt.

b) Unter Berücksichtigung der Art der Verarbeitung unterstützt der Auftragsverarbeiter den Verantwortlichen bei der Erfüllung von dessen Pflicht, Anträge betroffener Personen auf Ausübung ihrer Rechte zu beantworten. Bei der Erfüllung seiner Pflichten gemäß den Buchstaben a und b befolgt der Auftragsverarbeiter die Weisungen des Verantwortlichen.

c) Abgesehen von der Pflicht des Auftragsverarbeiters, den Verantwortlichen gemäß Klausel 8 Buchstabe b zu unterstützen, unterstützt der Auftragsverarbeiter unter Berücksichtigung der Art der Datenverarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen zudem bei der Einhaltung der folgenden Pflichten:

1) Pflicht zur Durchführung einer Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten (im Folgenden „Datenschutz-Folgenabschätzung"), wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat;
2) Pflicht zur Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft;
3) Pflicht zur Gewährleistung, dass die personenbezogenen Daten sachlich richtig und auf dem neuesten Stand sind, indem der Auftragsverarbeiter den Verantwortlichen unverzüglich unterrichtet, wenn er feststellt, dass die von ihm verarbeiteten personenbezogenen Daten unrichtig oder veraltet sind;
4) Verpflichtungen gemäß Artikel 32 der Verordnung (EU) 2016/679.

d) Die Parteien legen in Anhang III die geeigneten technischen und organisatorischen Maßnahmen zur Unterstützung des Verantwortlichen durch den Auftragsverarbeiter bei der Anwendung dieser Klausel sowie den Anwendungsbereich und den Umfang der erforderlichen Unterstützung fest.

9. Klausel 9: Meldung von Verletzungen des Schutzes personenbezogener Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten arbeitet der Auftragsverarbeiter mit dem Verantwortlichen zusammen und unterstützt ihn entsprechend, damit der Verantwortliche seinen Verpflichtungen gemäß den Artikeln 33 und 34 der Verordnung (EU) 2016/679 oder gegebenenfalls den Artikeln 34 und 35 der Verordnung (EU) 2018/1725 nachkommen kann, wobei der Auftragsverarbeiter die Art der Verarbeitung und die ihm zur Verfügung stehenden Informationen berücksichtigt.

9.1. Verletzung des Schutzes der vom Verantwortlichen verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Verantwortlichen verarbeiteten Daten unterstützt der Auftragsverarbeiter den Verantwortlichen wie folgt:

a) bei der unverzüglichen Meldung der Verletzung des Schutzes personenbezogener Daten an die zuständige(n) Aufsichtsbehörde(n), nachdem dem Verantwortlichen die Verletzung bekannt wurde, sofern relevant (es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen);

b) bei der Einholung der folgenden Informationen, die gemäß Artikel 33 Absatz 3 der Verordnung (EU) 2016/679 in der Meldung des Verantwortlichen anzugeben sind, wobei diese Informationen mindestens Folgendes umfassen müssen:

1) die Art der personenbezogenen Daten, soweit möglich, mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
2) die wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
3) die vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt;

c) bei der Einhaltung der Pflicht gemäß Artikel 34 der Verordnung (EU) 2016/679, die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten zu benachrichtigen, wenn diese Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

9.2. Verletzung des Schutzes der vom Auftragsverarbeiter verarbeiteten Daten

Im Falle einer Verletzung des Schutzes personenbezogener Daten im Zusammenhang mit den vom Auftragsverarbeiter verarbeiteten Daten meldet der Auftragsverarbeiter diese dem Verantwortlichen unverzüglich, nachdem ihm die Verletzung bekannt wurde. Diese Meldung muss zumindest folgende Informationen enthalten:

a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und der ungefähren Zahl der betroffenen Datensätze);

b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung des Schutzes personenbezogener Daten eingeholt werden können;

c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Wenn und soweit nicht alle diese Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen, und weitere Informationen werden, sobald sie verfügbar sind, anschließend ohne unangemessene Verzögerung bereitgestellt.

Die Parteien legen in Anhang III alle sonstigen Angaben fest, die der Auftragsverarbeiter zur Verfügung zu stellen hat, um den Verantwortlichen bei der Erfüllung von dessen Pflichten gemäß Artikel 33 und 34 der Verordnung (EU) 2016/679 zu unterstützen.

III. ABSCHNITT III

SCHLUSSBESTIMMUNGEN

10. Klausel 10: Verstöße gegen die Klauseln und Beendigung des Vertrags

a) Falls der Auftragsverarbeiter seinen Pflichten gemäß diesen Klauseln nicht nachkommt, kann der Verantwortliche – unbeschadet der Bestimmungen der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 – den Auftragsverarbeiter anweisen, die Verarbeitung personenbezogener Daten auszusetzen, bis er diese Klauseln einhält oder der Vertrag beendet ist. Der Auftragsverarbeiter unterrichtet den Verantwortlichen unverzüglich, wenn er aus welchen Gründen auch immer nicht in der Lage ist, diese Klauseln einzuhalten.

b) Der Verantwortliche ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn

1) der Verantwortliche die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter gemäß Buchstabe a ausgesetzt hat und die Einhaltung dieser Klauseln nicht innerhalb einer angemessenen Frist, in jedem Fall aber innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;

2) der Auftragsverarbeiter in erheblichem Umfang oder fortdauernd gegen diese Klauseln verstößt oder seine Verpflichtungen gemäß der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 nicht erfüllt;

3) der Auftragsverarbeiter einer bindenden Entscheidung eines zuständigen Gerichts oder der zuständigen Aufsichtsbehörde(n), die seine Pflichten gemäß diesen Klauseln, der Verordnung (EU) 2016/679 und/oder der Verordnung (EU) 2018/1725 zum Gegenstand hat, nicht nachkommt.

c) Der Auftragsverarbeiter ist berechtigt, den Vertrag zu kündigen, soweit er die Verarbeitung personenbezogener Daten gemäß diesen Klauseln betrifft, wenn der Verantwortliche auf der Erfüllung seiner Anweisungen besteht, nachdem er vom Auftragsverarbeiter darüber in Kenntnis gesetzt wurde, dass seine Anweisungen gegen geltende rechtliche Anforderungen gemäß Klausel 7.1 Buchstabe b verstoßen.

d) Nach Beendigung des Vertrags löscht der Auftragsverarbeiter nach Wahl des Verantwortlichen alle im Auftrag des Verantwortlichen verarbeiteten personenbezogenen Daten und bescheinigt dem Verantwortlichen, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Verantwortlichen zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragsverarbeiter weiterhin die Einhaltung dieser Klauseln.

AI ANHANG I

LISTE DER PARTEIEN

Verantwortlicher:
[Name und Anschrift des Kunden]
Unterschrift und Beitrittsdatum

VIDEC Data Engineering GmbH Contrescarpe 1 28203 Bremen Fon: (0421) 33950 – 0 Fax: (0421) 33950 – 50 E-Mail: info@videc.de	Datenschutzbeauftragter des Auftragsverarbeiters Dr. Andreas Melzer kelobit IT-Experts GmbH Thüringer Str. 31 06112 Halle (Saale) Fon: 0345 132553-80 E-Mail: datenschutz@kelobit.de
Unterschrift und Beitrittsdatum	

AII ANHANG II

BESCHREIBUNG DER VERARBEITUNG

Kategorien betroffener Personen, deren personenbezogene Daten verarbeitet werden	• Beschäftigte des Verantwortlichen • Bereitschafts- und Servicepersonal des Verantwortlichen • Beschäftigte von Dienstleistern des Verantwortlichen • Externe Kontaktpersonen des Verantwortlichen
Kategorien personenbezogener Daten, die verarbeitet werden	• Stammdaten (Name, Funktion) • Dienstliche Kontaktdaten (Telefon, E-Mail) • Benutzerkennungen und Berechtigungen in den Softwareprodukten • Protokoll- und Ereignisdaten (Anmeldungen, Bedienhandlungen, Quittierungen, Zeitstempel) • Kontaktdaten von Alarm- und Meldungsempfängern (Name, Telefon, E-Mail, Bereitschaftszeiten) • Sonstige Inhalte, die der Verantwortliche im Einzelfall überlässt
Verarbeitete sensible Daten	Keine. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sowie Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO sind nicht Gegenstand der Verarbeitung.
Art der Verarbeitung	• Kenntnisnahme personenbezogener Daten in den Systemen des Verantwortlichen bei Einrichtung, Konfiguration, Aktualisierung, Wartung und Support der Softwareprodukte Zugriff vor Ort oder per Fernzugriff, jeweils auf Anforderung und nach Freigabe durch den Verantwortlichen • Entgegennahme und Speicherung von Daten, die der Verantwortliche im Einzelfall auf dokumentierte Weisung übermittelt (z. B. Fehlerberichte, Logdateien, Datenbankauszüge), bis zum Abschluss des Vorgangs • Erfassen und Anlegen von Daten bei Einrichtung und Konfiguration • Ansehen und Auslesen von Daten bei Analyse und Fehlersuche • Verändern von Daten im Rahmen der Fehlerbehebung • Übernahme von Daten in das Ticketsystem des Auftragsverarbeiters, soweit für die Analyse erforderlich • Ändern von Einstellungen in den Softwareprodukten auf Anweisung des Verantwortlichen • Löschen von Daten auf Weisung des Verantwortlichen oder nach Abschluss des Vorgangs
Zweck(e), für den/die die personenbezogenen Daten im Auftrag des Verantwortlichen verarbeitet werden	• Einrichtung, Konfiguration und Inbetriebnahme der vom Verantwortlichen eingesetzten Softwareprodukte • Unterstützung bei Updates und Wartung der Softwareprodukte • Anwendungssupport für die Beschäftigten des Verantwortlichen • Fehlerdiagnose und Fehlerbehebung zur Sicherstellung der Betriebsbereitschaft • Unterstützung bei der Bewertung der OT-Umgebung im Netzwerk des Verantwortlichen • Einbindung des jeweiligen Herstellers im 3rd-Level-Support nach Anhang IV, sofern erforderlich
Dauer der Verarbeitung	• Während der gesamten Dauer der Leistungsvereinbarung, der Lizenzierung oder eines Wartungsvertrags • Im Einzelfall übermittelte Daten und Kopien im Ticketsystem werden spätestens sechs Monate nach Abschluss des jeweiligen Vorgangs gelöscht, sofern keine gesetzliche Aufbewahrungspflicht besteht, auf Verlangen des Verantwortlichen früher • Nach Beendigung des Vertrags Löschung oder Rückgabe der Daten gemäß Klausel 10 Buchstabe d
Gegenstand, Art und Dauer der Verarbeitung bei Unterauftragsverarbeitern	• 3rd-Level-Support des jeweiligen Herstellers, sofern erforderlich, sowie Fernwartung, Kommunikation und Ticketsystem über die eingesetzten Dienstanbieter, Einzelheiten je • Unterauftragsverarbeiter in Anhang IV Dauer wie beim Auftragsverarbeiter, im Einzelfall übermittelte Daten höchstens bis zum Abschluss des jeweiligen Vorgangs beim Hersteller

AIII ANHANG III

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN, EINSCHLIEßLICH ZUR GEWÄHRLEISTUNG DER SICHERHEIT DER DATEN

Beschreibung der vom Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

1. Grundsatz der Verarbeitung von Supportdaten
   - Tiefergehende Analysen, für die Daten von Systemen des Verantwortlichen auf Systeme von VIDEC und gegebenenfalls des Herstellers übertragen werden, führt VIDEC ausschließlich auf Weisung in Textform und nach vorheriger Genehmigung durch den Verantwortlichen durch.
   - Typische Daten sind Datenbank-Dumps bzw. Exporte, Kundendaten aus zentralen CRM-Systemen und komplexe Daten über Systemzustände.
   - VIDEC hält diese Daten am Vorgang im Ticketsystem vor, entweder in Odoo auf eigenen Servern oder in Jira beim Unterauftragsverarbeiter Atlassian nach Anhang IV, und löscht sie spätestens sechs Monate nach Abschluss des Vorgangs, sofern keine gesetzliche Aufbewahrungspflicht besteht, auf Verlangen des Verantwortlichen früher.
   - Für die Dauer der Verarbeitung liegen alle Daten des Verantwortlichen in einem gesicherten, nur für ihn bestimmten logischen Bereich. Der Zugriff ist auf berechtigte Personen beschränkt.

2. Pseudonymisierung und Verschlüsselung
   - Datenübermittlung ausschließlich über verschlüsselte Verbindungen (VPN/TLS)
   - Verschlüsselung lokal gespeicherter Daten
   - Verschlüsselte Speicherung von Passwörtern
   - Eine Pseudonymisierung erfolgt nicht, weil die Verarbeitung anlassbezogen und streng zweckgebunden ist.

3. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
   - Zugriffskontrolle nach festgelegtem Berechtigungskonzept mit differenzierten Berechtigungen
   - Zugriff ausschließlich über zugewiesene Berechtigungen, offene Benutzergruppen bestehen nicht
   - Trennung von System- und Benutzerdateien sowie der Benutzerdateien verschiedener Benutzer
   - Zweckgebundene, getrennte Speicherung (z. B. Test- und Produktionsumgebung)
   - Trennung von Daten anderer Auftraggeber (Mandantenfähigkeit)
   - Virenabwehr mit automatischer regelmäßiger Aktualisierung

4. Wiederherstellung von Verfügbarkeit und Zugang
   - Datensicherungskonzept für personenbezogene Daten, Anwendungsprogramme und Systemumgebung
   - Ausschließliche Verwendung hochwertiger Datenträger
   - Einfache Wiederherstellung einzelner Dateien bei sichergestellter Verfügbarkeit von Sicherungsdaten und Infrastruktur
   - Sicherungsdatenträger unter Verschluss, zugänglich nur für beauftragte Systemadministratoren
   - Datensicherungen an unterschiedlichen Örtlichkeiten

5. Regelmäßige Überprüfung, Bewertung und Evaluierung
   - Protokolldaten sind gegen Manipulation geschützt und werden gelöscht, sobald sie nicht mehr benötigt werden
   - Verzeichnis der eingesetzten IT-Geräte sowie Dokumentation der Hardware einschließlich Netzanbindung
   - Schriftliche Arbeitsanweisungen, die allen an der Verarbeitung beteiligten Mitarbeitenden bekannt sind und geschult werden

6. Identifizierung und Autorisierung der Nutzer
   - Vergabe von Benutzerrechten ausschließlich durch Systemadministratoren
   - Eigenes Benutzerkonto je natürlicher Person
   - Anmeldung mit Benutzerkennung und Passwort
   - Erzwungene Passwortregeln: Wechsel des Erstpassworts, Mindestlänge 8 Zeichen, Zurückweisung unsicherer Passwörter
   - Zeitliche Begrenzung der Passwortgültigkeit
   - Zwei-Faktor-Authentifizierung
   - Verschlüsselte Passwortspeicherung
   - Protokollierung von Anmeldungen und Fehlversuchen
   - Automatische Sperrung nach wiederholten Fehlversuchen
   - Zuordnung von Benutzern zu bestimmten Arbeitsplätzen
   - Passwortgeschützter Bildschirmschoner

7. Schutz der Daten bei Übermittlung und Speicherung
   - Verschlüsselter Datentransfer (VPN/TLS)
   - Datenträger und Unterlagen stets unter Verschluss, Zugang nur für einen festgelegten Kreis von Berechtigten
   - Vollständige physikalische Löschung von Datenträgern nach dem Stand der Technik vor Wiederverwendung oder Entsorgung
   - Datenschutzkonforme Entsorgung von Ausdrucken und Akten, sobald der Verwendungszweck entfällt
   - Verschlüsselung lokal gespeicherter Daten

8. Physische Sicherheit und Protokollierung

   Standort Contrescarpe 1, 28203 Bremen, in eigenen, gekennzeichneten VIDEC-Räumen. Die Netzwerkleitungen laufen im Serverraum zusammen und sind von fremden Räumen getrennt.
   - Überwachungseinrichtung mit Alarmanlage und Videomonitor
   - Türsicherung mit persönlichen Schlüsseln, elektrischen Türöffnern und individuellem Einlass
   - Abschließbare Räume, Rechnerschränke und Geräte
   - Zutritt ausschließlich nach Zutrittsregelung
   - Bildschirme außerhalb des Blickfelds Unbefugter
   - Abhörsichere Kabelverlegung

9. Systemkonfiguration, interne Governance und IT-Sicherheit
   - Interne Governance über schriftliche, geschulte Arbeitsanweisungen
   - Verzeichnis der eingesetzten IT-Geräte sowie Hardware- und Netzdokumentation
   - Virenabwehrprogramme mit automatisierter regelmäßiger Aktualisierung

10. Datenminimierung und datenschutzfreundliche Voreinstellungen
    - Datenminimierung und Zweckbindung sind etabliert.
    - Voreinstellungen begrenzen die Verarbeitung personenbezogener Daten auf das für den Zweck Erforderliche.

11. Datenqualität
    - Die Verarbeitung erfolgt anlass- und zweckgebunden, Daten werden höchstens sechs Monate nach Abschluss des Vorgangs gehalten.
    - Stellt VIDEC fest, dass Daten unrichtig oder veraltet sind, unterrichtet VIDEC den Verantwortlichen unverzüglich.

12. Begrenzte Speicherung und Rechenschaftspflicht
    - Im Einzelfall übermittelte Supportdaten werden am Vorgang im Ticketsystem vorgehalten und spätestens sechs Monate nach Abschluss des Vorgangs gelöscht.
    - Auf Verlangen des Verantwortlichen erfolgt die Löschung früher und wird ihm in Textform bestätigt.

13. Datenübertragbarkeit und Löschung
    - Bei Vertragsende Löschung oder Rückgabe der Daten nach Wahl des Verantwortlichen
    - Bestätigung der Löschung bei Vertragsende und auf Verlangen des Verantwortlichen
    - Physikalische Löschung von Datenträgern nach dem Stand der Technik

14. Unterstützung des Verantwortlichen
    - Unterstützung bei der Wahrung der Betroffenenrechte
    - Konzept zur Meldung von Datenschutzverletzungen
    - Mitarbeitende sind dokumentiert über Meldewege und Notfallpläne informiert
    - Der Verantwortliche wird unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis, über Datenschutzverletzungen informiert

15. Fernzugriff
    - Fernzugriff erfolgt nur über einen vom Verantwortlichen freigegebenen, gesicherten Zugangsweg
    - Jede Sitzung wird im Einzelfall vom Verantwortlichen gestartet oder freigegeben
    - Der Verantwortliche kann die Sitzung beobachten und jederzeit beenden
    - Eingesetztes Fernwartungswerkzeug ist TeamViewer, in Projekten alternativ ein VPN- oder RDP-Zugang des Verantwortlichen

AIV ANHANG IV

LISTE DER UNTERAUFTRAGSVERARBEITER

Der Verantwortliche hat die Inanspruchnahme folgender Unterauftragsverarbeiter genehmigt:

1	dataforum Software GmbH Friedrich-Ebert-Straße 53 34266 Niestetal Sylvester Weise (Geschäftsführer) Tel.: +49 561 52 85 66 E-Mail: info@dataforum.de	Hersteller des Produkts acron, sofern 3rd-Level-Support erforderlich: • Analyse von Fehlerberichten, ggf. Logdateien • Übermittlung, Prüfung, Nutzung von Datenbanken zur Nachstellung und Behebung von Fehlern • Fernzugriff/Fernwartung zur Fehlerbehebung auf Wunsch des und nach Freigabe durch den Verantwortlichen
2	Achtwerk GmbH & Co KG Am Mohrenshof 11a 28277 Bremen Jens Bußjäger, Stefan Menge (Geschäftsführer) Tel.: +49 421 878 478 80 E-Mail: kontakt@acht-werk.de	Hersteller des Produkts IRMA, sofern 3rd-Level-Support erforderlich: • Analyse von Fehlerberichten, ggf. Logdateien • Übermittlung, Prüfung, Nutzung von Datenbanken zur Nachstellung und Behebung von Fehlern • Fernzugriff/Fernwartung zur Fehlerbehebung auf Wunsch des und nach Freigabe durch den Verantwortlichen
3	InnovatePro Management Italy S.R.L. (Hersteller der Proficy-Produkte, vormals GE Vernova) Piazza Borgo Pila 39 16129 Genua, Italien Luigi Neri (Company Legal Representative) E-Mail: innovatepro.italy@legalmail.it	Hersteller der Proficy-Produkte, sofern 3rd-Level-Support erforderlich: • Analyse von Fehlerberichten, ggf. Logdateien • Übermittlung, Prüfung, Nutzung von Datenbanken zur Nachstellung und Behebung von Fehlern • Fernzugriff/Fernwartung zur Fehlerbehebung auf Wunsch des und nach Freigabe durch den Verantwortlichen • Bearbeitung ausschließlich in der EU, eine Übermittlung in Drittländer findet nicht statt
4	TeamViewer Germany GmbH Bahnhofsplatz 2 73033 Göppingen	Anbieter der Fernwartungssoftware TeamViewer: • Herstellen der Fernwartungsverbindung auf Wunsch des und nach Freigabe durch den Verantwortlichen • Verbindungs- und Protokolldaten der Sitzung, Kenntnisnahme von Bildschirminhalten
5	Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park Leopardstown, Dublin 18, Irland	Anbieter von Microsoft 365 (Teams, Exchange Online): • Videokonferenzen mit Bildschirmfreigabe im Support Empfang und Speicherung von Supportdaten per E-Mail • Drittlandsübermittlung an Microsoft Corporation (USA) möglich (Grundlage: Abschluss Standardvertragsklauseln, Angemessenheitsbeschluss für USA, DPF-Zertifizierung für Microsoft vorhanden)
6	Atlassian Pty Ltd Level 6, 341 George Street Sydney NSW 2000, Australien	Anbieter des Ticketsystems Jira: • Speicherung von Supportdaten am Vorgang bis zur Löschung nach Anhang III Nr. 1 • Drittlandsübermittlung nach Australien und in die USA möglich (Grundlage: Abschluss sind die Standardvertragsklauseln, Angemessenheitsbeschluss für Australien und USA, DPF-Zertifizierung für Atlassian vorhanden)